AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEIZURE WARRANT

I, Justin Woodford, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation and have been since January 2021. Since becoming a Special Agent, I have been assigned to a Cyber Crime Task Force in Albany, NY. I am responsible for investigating complex criminal computer intrusions and cyber fraud, including fraud involving cryptocurrency. I have experience working ransomware, business email compromise, and cryptocurrency trading platform fraud cases, commonly known as "Pig Butchering". I have received training related to cyber security, open-source intelligence, and reverse malware engineering and have a bachelor's degree in computer and information science. I have participated in the execution of search warrants involving electronic evidence, including searches of email accounts and computers.

2. This affidavit is offered to demonstrate that probable cause to believe that the Tether (USDT) held in the Target Wallets listed below (hereinafter the "TARGET PROPERTY") represents funds involved in and the proceeds of a wire fraud and money laundering scheme and is thus civilly forfeitable to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) and (a)(1)(C) and subject to seizure via a civil seizure warrant by 18 U.S.C. § 981(b)(1), and is criminally forfeitable pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c) and 18 U.S.C. § 982(a)(1) and subject to a criminal seizure warrant pursuant to 21 U.S.C. § 853(e) by 28 U.S.C. § 2461(c) and 21 U.S.C. § 853(e) and (f) by 18 U.S.C. § 982(b)(1).The TARGET PROPERTY is described here and in Attachment A as:

Tether (USDT) held in the following Target Wallets, with the listed balances as of July 26, 2024 (for a total of 1,897,169.648281 USDT across two networks, Ethereum (ETH) and Tron (TRX)):

i. Target Wallet 1 (0x74530e81E9f4715c720b6b237f682CD0e298B66C): USDT/ETH 1,359,253.29346
ii. Target Wallet 2 (TEDNf1aqk8YJEUdNH9NRd4MqibZmdP49Fm): USDT/TRX 537,916.354821

3. The information contained in this affidavit is based upon my training, my experience, my own investigation, and my conversations with other law enforcement officers involved in the investigation. The following is either known to me personally or has been relayed to me by persons having direct knowledge of the events described below. It is meant to set forth probable cause and does not include every fact known to law enforcement about the events described below.

Background on Tether

4. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. Dollar, or to a different virtual currency. For example, USDC is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

5. **Tether (USDT)**: "TetherUS" (USDT), also referred to as "Tether," is a cryptocurrency purportedly backed by United States dollars. Tether was originally designed to always be worth $1, and the company responsible for issuing Tether purportedly maintained $1 in reserves for each Tether issued. As of January 1, 2024, one Tether coin was worth approximately $1 USD. Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (*i.e.,* the funds held in reserve) for USDT tokens.

Probable Cause

6. On or around September 14, 2023, a cyber-attack at Remitano, a cryptocurrency exchange registered in Vilnius, Lithuania as UAB Retech Labs, with international customers

including in the United States, led to the theft of virtual assets across multiple networks. According to reports of the theft, an unknown cyber actor redirected virtual assets from Remitano's accounts into accounts associated with the theft scheme.

7. The FBI reviewed blockchain data and observed the following transactions of USDT leaving Remitano:

a. On September 14, 2023 at 13:07 UTC, transaction hash 04f3103388a311db69c5b301c675f7fe1a847d9fb1a1edaf0d98950ecf37b14b, where 69,694.5122 USDT/TRX was observed sent from TLYCaS9cZErMpUuwjZQbkFvYqx6Zaq11hE (Remitano's hot wallet[1]) to TEDNf1aqk8YJEUdNH9NRd4MqibZmdP49Fm (Target Wallet 2).

b. On September 14, 2023 at 12:36 UTC, transaction hash f29c1ebf6f62a180b3c0d6fc0a299c12c989efaf8edc74a9da5a6553f6ee923c, where 468,221.842621 USDT/TRX was observed sent from TLYCaS9cZErMpUuwjZQbkFvYqx6Zaq11hE (Remitano's hot wallet) to TEDNf1aqk8YJEUdNH9NRd4MqibZmdP49Fm (Target Wallet 2).

c. On September 14, 2023 at 12:45 UTC, transaction hash 0xe0725362fd774de0d8416d5e3d028063508ffa61f68087c576320e42159677a9, where 1,359,253.29346 USDT/ETH was observed sent from 0x2819c144D5946404C0516B6f817a960dB37D4929 (Remitano's hot wallet) to 0x74530e81E9f4715c720b6b237f682CD0e298B66C (Target Wallet 1).

[1] Hot wallets are cryptocurrency wallets with a connection to the internet. This allows the administrator of the wallet to make transactions more quickly on the blockchain. This type of wallet is optimal for larger volumes of transactions. At an exchange such as Remitano, the hot wallet facilitates transactions for all its users.

8. The United States Attorney's Office in the District of Vermont, the Federal Bureau of Investigation, and other private entities requested Tether to voluntarily restrain the TARGET PROPERTY such that Tether in Target Wallet 1 and Target Wallet 2 could not further transact with the USDT contract on the Tron network (TRX) and Ethereum network (ETH). On September 14, 2023, Tether reviewed the request and agreed to prevent further movement of the Target Property.

9. On or around July 15, 2024, a representative of the legal team at Remitano contacted the FBI. The representative stated that Remitano hired a third-party company, CryptoForensic Investigators, to investigate the event and assist in the recovery efforts of the stolen assets. CryptoForensic Investigators concluded that a security breach occurred at Remitano because of a vulnerability in a third-party service that ultimately led the theft of cryptocurrency from the Remitano exchange hot wallet. The representative confirmed that the transactions the FBI observed moving into the Target Wallets were not initiated by or for Remitano and represented movement of funds involved in, and the proceeds of, the crime.

10. The foregoing establishes probable cause to believe that the TARGET PROPERTY is subject to civil and criminal forfeiture, as it is associated with wire fraud and money laundering, namely the virtual intrusion by an unknown actor into systems that allowed the actor to access Remitano's funds and the subsequent movement of those funds into other wallets, potentially to obscure the source of the funds and make the funds harder to trace.[2] Should this seizure warrant be granted, law enforcement intends to work with Tether to seize the funds

[2] While in this instance, the FBI sought Tether's agreement to voluntarily restrain the Target Property on the day of the theft, had the FBI not brought the crime to Tether's attention, the funds would likely have been further diluted before law enforcement could track or recover them.

associated with the TARGET PROPERTY. In sum, the accompanying warrant would be transmitted to Tether, at which time Tether would "burn" (*i.e.*, destroy) the addresses at issue (and by extension the USDT tokens associated with them). Tether would then reissue the equivalent amount of USDT tokens associated the TARGET PROPERTY and transfer that equivalent amount of USDT to a government-controlled wallet. The seized currency will remain in the custody of the U.S. government during the entire pendency of the forfeiture proceedings, to ensure that access to, or manipulation of, the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

11. Because this warrant seeks only permission to seize funds held by Tether and does not involve the physical intrusion onto a premises, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Dated at Burlington, in the District of Vermont, this ____ day of July 2024.

/s/ Justin Woodford
Justin Woodford, FBI Special Agent

Sworn to by the applicant via reliable electronic means under Federal Rule of Criminal Procedure 4.1(b)(2)(A)—specifically, a video call—on this 30th day of July, 2024.

HON. KEVIN J. DOYLE
United States Magistrate Judge
District of Vermont